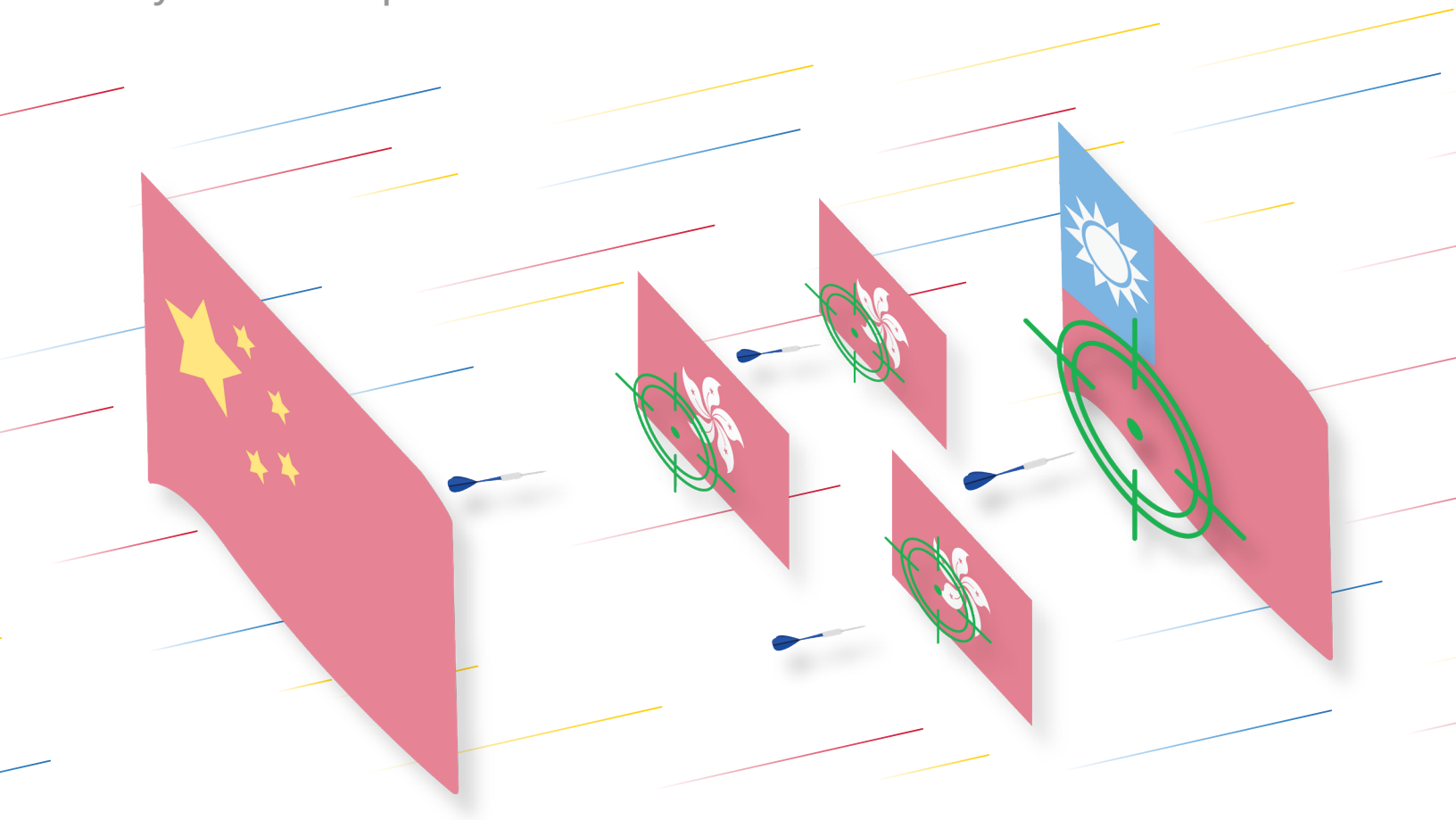
Recorded Future®

CYBER THREAT ANALYSIS | CHINA

Chinese Influence Operations Evolve in Campaigns Targeting Taiwanese Elections, Hong Kong Protests

By Insikt Group®



CTA-CH-2020-0429

Recorded Future analyzed data from the Recorded Future® Platform, social media sites, local and regional news sites, academic studies, information security reporting, and other open sources (OSINT) for updates on Chinese state-sponsored influence operations targeting the 2020 Taiwanese presidential elections and Hong Kong protests. This report covers topics and information from September 21, 2019 through March 20, 2020 and will be of most value to government departments, geopolitical scholars and researchers, and all users of social media.

Executive Summary

As outlined by previous Insikt Group research, Chinese influence operations often aim to present a positive, benign, and cooperative image of China to foreign audiences. However, we have discovered that there is a more aggressive and coercive side of Chinese influence operations when it comes to the targeting of Taiwan and Hong Kong, regions that China has long viewed as domestic territory.

This research focuses on emerging tactics, techniques, and procedures (TTPs) that Chinese state-affiliated or state-friendly actors have deployed in campaigns targeting the 2020 Taiwan presidential election and the 2019-2020 Hong Kong protests. In the context of Taiwan, we observed Chinese state-affiliated activities stealthily targeting every segment of the influence operations lifecycle, from production and amplification to dissemination. With respect to the 2019 Hong Kong protests, we observed new attack methods, infrastructure, and grassroot groups being deployed in nontraditional ways to defend and promote Chinese nationalistic propaganda and state interests.

Key Judgments

- We assess that content farms will continue to play a leading role in enabling mainland Chinese disinformation efforts targeting Taiwan.
- Taiwan's unique efforts to discover, identify, and counter Chinese state-sponsored influence operations will likely force Chinese influencers to innovate and use more covert operational TTPs. We believe that these new tactics will likely include recruitment of overseas Chinese nationals, co-option of Taiwanese content farms and social media influencers, use of cover organizations, procurement of aged social media accounts, and more.

- We assess that Chinese influence operators will likely employ artificial intelligence (AI) and bulk social media management software to ease the propagation of weaponized content at scale, especially on closed messaging platforms such as LINE or WhatsApp. Western social media platforms will also be likely targets for such automated campaigns during sensitive periods such as elections and global events, on issues that are relevant to China's national image and state interests.
- We judge that China will seek to identify local collaborators in Taiwan and Hong Kong, or those with policy or political views sympathetic to China, such as public figures, politicians, and marketing firms, to obfuscate China as the information source and increase its perceived authenticity.
- We assess that new TTPs used to target Hong Kong protesters — crowd-sourced doxxing of anti-government protesters and social media "rallies" to support Chinese state interests — are likely to become regularly deployed tools in Chinese domestic and overseas influence operations.
- We assess that the Chinese government is likely to start leveraging the existing patriotism and capabilities of online grassroot groups to promote and defend state interests abroad through explicit direction and implicit nudging.

Background

Taiwan and Hong Kong have long been geopolitical flashpoints for the mainland Chinese government, which has struggled to build and maintain a legitimate standing with the people of these two special-status "regions," both of which Beijing views as its sovereign territory and key elements of overall domestic stability.

From a tactical standpoint, the mainland Chinese government views both Taiwan and Hong Kong as domestic information space. As a result, it is not unusual to observe active Chinese intelligence and influence tactics in use that have not been traditionally employed in other foreign spaces.

In this research, Insikt Group focuses on new TTPs that have been used to target the most important political events in Taiwan and Hong Kong this past year — namely, the 2020 Taiwan presidential elections, which were held on January 11, 2020, and the series of large-scale Hong Kong protests that started in June 2019 in reaction to the 2019 Hong Kong Extradition Bill. The data sets we used were from September 21, 2019 through March 20, 2020 for the Hong Kong protests, and from October 1, 2019 through January 22, 2020 for the Taiwanese elections.

Taiwan's 2020 Presidential Elections

Recorded Future observed a spike in references to "disinformation," "fake news," and "influence operations" in the context of Taiwan between October 2019 and January 2020. In the first half of January alone, our analysts observed 1,223 references, compared with the 775 references observed in December 2019, with peak volume immediately following the Taiwanese presidential elections on January 11, 2020, in which incumbent president Tsai Ing-wen successfully won a second term.

Despite the conclusion of the 2020 Taiwanese election cycle and the subsequent drop in references to disinformation campaigns and fake news targeting Taiwan, Recorded Future assesses it is highly likely that Chinese influence operations aimed at dividing Taiwanese society and promoting pro-China narratives and political candidates persist. Beijing has adopted this approach toward Taiwan since President Tsai of Taiwan's Democratic Progressive Party (DPP)[1] first unseated the pro-China Kuomintang (KMT, the Chinese Nationalist Party) in 2016.

However, it is important to note that different parties in Taiwan also engage in online campaigns to sway public opinion to their respective interests, some of which are aligned with Chinese Communist Party (CCP) interests and employ similar TTPs. This convergence in interests, policy goals, and TTPs occasionally presents difficulties in distinguishing between Chinese (mainland) interference activity and Taiwanese political activity. We distinguish between the two types of activities to the best of our knowledge in the following analysis.

[1] The DPP is one of two major political parties in Taiwan, and has been traditionally associated with promoting human rights, anti-communism, a distinct Taiwanese identity, and Taiwan's sovereignty.

Covert Influence

This section describes TTPs used by Chinese covert influence operators to target Taiwanese users across Facebook, the popular messaging app LINE, and YouTube. We also assess the role and impact of Chinese content farms in the disinformation supply chain targeting Taiwan, and highlight associated TTPs:

- **Content Farms**: Publishing fake news stories in English, AI-generated content, and China-friendly Taiwanese content farms
- **Facebook**: Employment of PR firms for Facebook influence operations, recruitment of Taiwanese influencers, and the use of Chinese software for monitoring and batch posting
- **LINE**: Use of Chinese software for monitoring and batch posting
- **YouTube**: Use of Chinese influencers to shape narratives on Taiwanese affairs, and the recruitment of Taiwanese YouTube influencers

Content Farms

Chinese and Taiwanese content farms[2] have become one of the biggest sources for misleading, intentionally biased, and false content in Taiwan. According to the database of Taiwanese fact-checking website MyGoPen (which translates to "don't lie" in Taiwanese), at least 60% of false or misleading information forwarded to the site are from foreign sources, the majority of which are from mainland China. Oftentimes, Taiwanese content farms also source content from Chinese sources, including Chinese content farms, Weibo posts, WeChat posts, and Chinese state media or state-affiliated platforms.

[2] We make a distinction between Chinese-originated and Taiwanese-originated content farms. Either may propagate material in simplified or traditional Chinese, or in any number of dialects, so the key factor in our determination is who the owners and/or operators are.

Aside from common tactics to generate internet traffic from Taiwanese users, such as crafting sensational titles for news articles copied from local news outlets, Taiwanese researcher Puma Shen has observed an evolution of tactics, with Chinese operators creating English-language content farms. In these content farms, English articles are first translated to written simplified Chinese and then to traditional Chinese (the official written characters of Hong Kong and Taiwan, rather than the simplified Chinese characters used by mainland Chinese) before being disseminated to Taiwanese users. We believe this evolution is likely for the purpose of deceiving the growing pool of Taiwanese internet users who have learned to verify news sources.

While we have not observed instances of content from English-language content farms being disseminated to Western audiences, we assess that such infrastructure and English-language content creation capabilities could be leveraged to target Western audiences.

Another emerging tactic used by both Chinese and Taiwanese content farms is the use of AI to generate massive volumes of content. In a May 2019 report on how to combat disinformation, Taiwan's Mainland Affairs Council — the agency responsible for China policy — speculated that China had been using AI technology in influence operations targeting Taiwan. This speculation was corroborated by Taiwanese online marketer and renowned public opinion manipulator Peng Kuan Chin (彭冠今). Peng created a "Content Farm Automatic Collection System" that crawls the internet for Chinese articles and posts and reorganizes the words and sentences into new text, generating thousands of articles per day. Peng's software is modeled on automation software he saw in China, which he believes no one else outside the mainland has.

Additionally, while Recorded Future has not observed evidence of Chinese manipulation of Taiwanese content farms, we assess that operators of popular Taiwanese content farms are likely to be seen as valuable assets for Chinese influence operations. One example is Lin Cheng Kuo (林正國), the owner and active contributor to one of Taiwan's most popular content farms, Mission (密訊).[3] Mission is one of the most shared sources on Facebook Taiwan (zh-tw.facebook[.]com), at times surpassing major local news outlets. Investigative news outlet

[3] The original Mission domain was mission-tw[.]com, but it has frequently changed domains to circumvent Facebook filters since being tagged as a content farm and banned from Facebook's News Feed in October 2019.

The Reporter recently revealed that Lin Cheng Kuo is an active member of Taiwan's New Party, which supports unification with Mainland China. Additionally, he has been photographed attending events held by China's provincial-level state-owned news station Hai Xia Dao Bao (海峡导报), alongside Chinese media personalities. We assess that, because popular Taiwanese content farms are so vital to spreading information to the Taiwanese public, owners and operators are likely to be seen as potential assets for Chinese influence operators.

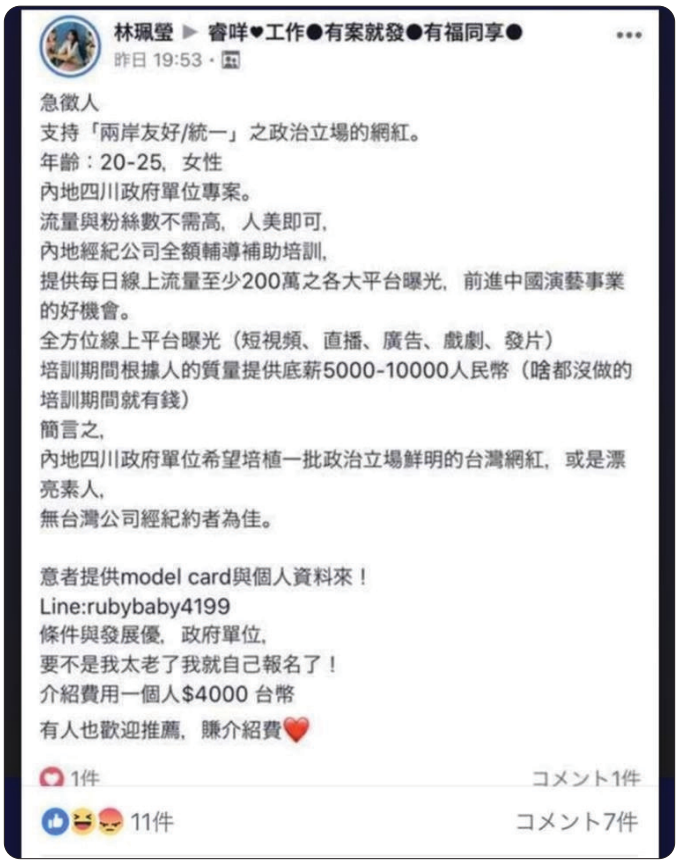
Facebook

Social media penetration in Taiwan is the highest in Asia, with 89% of the population using social media at least once per day. Facebook is one of the most popular social media outlets in Taiwan, with 89% of Taiwanese internet users reported to use the platform. Facebook has become a prime target for Chinese influence operations in Taiwan, probably because of its wide reach and product stickiness. According to Taiwanese researcher Puma Shen, many content farms have relied on Facebook "fan" pages to spread disinformation. However, many of these pages were banned or deleted in 2019, so content farmers have resorted to employing freelance individuals in Malaysia, or other overseas Chinese nationals, to disseminate the content farm's misleading content across Facebook. We assess that this trend toward employing more covert means of disseminating disinformation via local third parties on Facebook will accelerate as Facebook tightens enforcement of its content policies.

In the first half of 2019, multiple owners of popular Taiwanese Facebook fan pages disclosed screenshots of strangers attempting to purchase their fan pages. While speculation is rife on social and traditional media that the purchasers are mainland Chinese citizens, these attempts have not been directly attributed to Chinese nationals. However, according to the testimony of the owner of a Taiwanese online marketing firm that specializes in PTT[4] influence campaigns, other marketing firms in the industry are conducting Facebook influence campaigns on behalf of the CCP, mostly through disseminating images and short commentaries criticizing the current administration.

[4] PTT is the largest terminal-based bulletin board system (BBS) based in Taiwan.

Additionally, we have identified Chinese provincial governments recruiting "mainland-friendly, pro-unification" Taiwanese influencers through Facebook posts, with the aim of "training a group of Taiwanese influencers with distinct political affiliations." The listings are often posted on behalf of the Chinese government agencies by Taiwanese locals, with one listing offering a base salary of ¥5,000 to ¥10,000 RMB (approximately $730 to $1,460 USD).



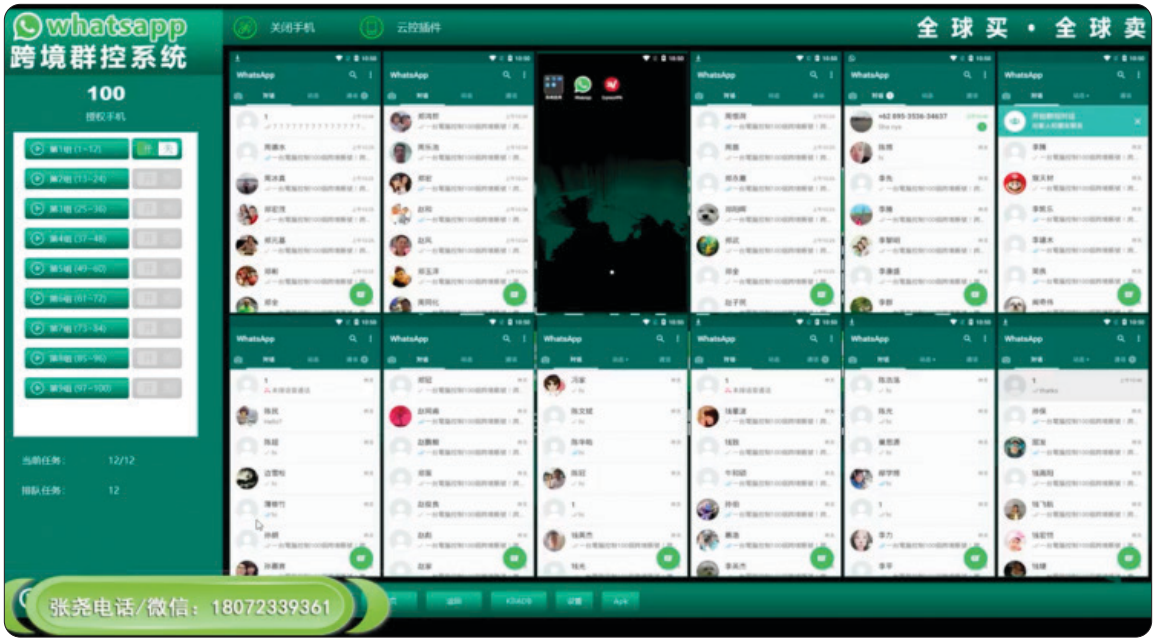
Facebook post recruiting Taiwanese influencers for the Sichuan government. (Source: HK01)

LINE

LINE is the most popular messaging app in Taiwan, with 21 million users (about 90% of Taiwan's population). According to research revealed by LINE in October 2019, Taiwanese users are unique in their love of using the "share" feature, which allows users to forward text, image, or video messages to other users and message groups within LINE. The share feature is used approximately a hundred million times per month by Taiwanese users, which is 40% of the total "shares" globally. This feature operates similarly to the "share" feature in WhatsApp, which is widely used by Indian nationals and has facilitated the mass dissemination of disinformation in India. We assess that the speed and breadth of sharing on LINE may render Taiwanese users particularly susceptible to Chinese influence operations.

Chinese operators may also benefit from social media management technologies, including a Chinese-developed software called "Cross-Border Cloud/Mass Management System" (跨境云/群控系统), which allows users to batch manage thousands of social media accounts at once (including Facebook, Instagram, WeChat, WhatsApp, LINE, QQ, and TikTok). The software allows users to breach the Great Firewall, change their IP addresses, batch create and translate posts (including converting written simplified Chinese content to traditional Chinese), batch manage groups, batch "like" and "share" posts, and more.

At this time, links between this software and mainland Chinese influence operations targeting Taiwan remain speculative and unsubstantiated; however, we believe that these technologies are likely currently being employed. That is because these technologies can ease the spread of weaponized content at scale, especially on closed messaging platforms such as LINE, where Taiwanese users frequently reshare content.



Screenshot of the cross-border cloud/mass management system UI for WhatsApp. (Source: Facebook)

YouTube

YouTube is also one of the most popular social media platforms in Taiwan, with 90% of Taiwanese internet users using the platform and 70% of those users visiting every day.

Researchers have observed that Chinese influence activity on YouTube has increased in 2019. 10 YouTube channels were created between August and October 2019 that all focused on attacking the administration of President Tsai Ing-wen. These researchers believe that some of the channels, which have more than 10,000 subscribers, are likely content farms run by Chinese nationals.

One example is the YouTube channel "Xida speaks on Taiwan at the foot of Yushan" (Yushan is the tallest mountain in Taiwan), which features China National Radio journalist and show host Zhang Xida (张希达). On the channel, Zhang attempts to speak Mandarin with a Taiwanese accent and comments on Taiwanese politics, mostly attacking the country's ruling DPP administration. China National Radio is the national radio station of China, and is under the purview of the Central Publicity Department of the CCP and the State Council of the People's Republic of China. The videos on the channel feature subtitles and graphics in traditional Chinese characters, which we assess is because the channel is highly likely to be targeting a Taiwanese audience. 15 videos were posted between August 23 and October 18, 2019, although the channel itself was created on August 3, 2014. At the time of this writing, the channel had 638,000 subscribers.

Xida's video titled "U.S. Interference of Taiwanese Elections — TAIPEI Act." (Source: YouTube)

Influence operations researcher Puma Shen has also observed advertisements listed by organizations affiliated with the United Front Work Department of the CCP (the agency responsible for coordinating influence operations to neutralize opposition to the CCP) recruiting Taiwanese YouTube influencers.

While none of these observed activities have been attributed directly to the CCP, Recorded Future assesses that we will see more Chinese and Taiwanese channels on YouTube promoting issues and political stances that are in the Chinese national interest in the few years leading up to the next Taiwanese presidential election.

Overt Influence

Between October 1, 2019 and January 22, 2020, Recorded Future observed 801 references to Taiwan, "Tsai Ing-wen," and "Han Kuo-yu" (the KMT presidential candidate) from the social media accounts of Chinese state-owned and state-affiliated media. Consistent with the roles of state media as mouthpieces of the CCP, messaging from these accounts falls into several major themes that are aligned with China's overall "carrot and stick" strategy towards Taiwan: criticism of the DPP administration and their policies, threats to deter Taiwanese independence or any deviation from the "One China" policy, and promotion of economic and cultural opportunities that come with closer cross-strait ties.

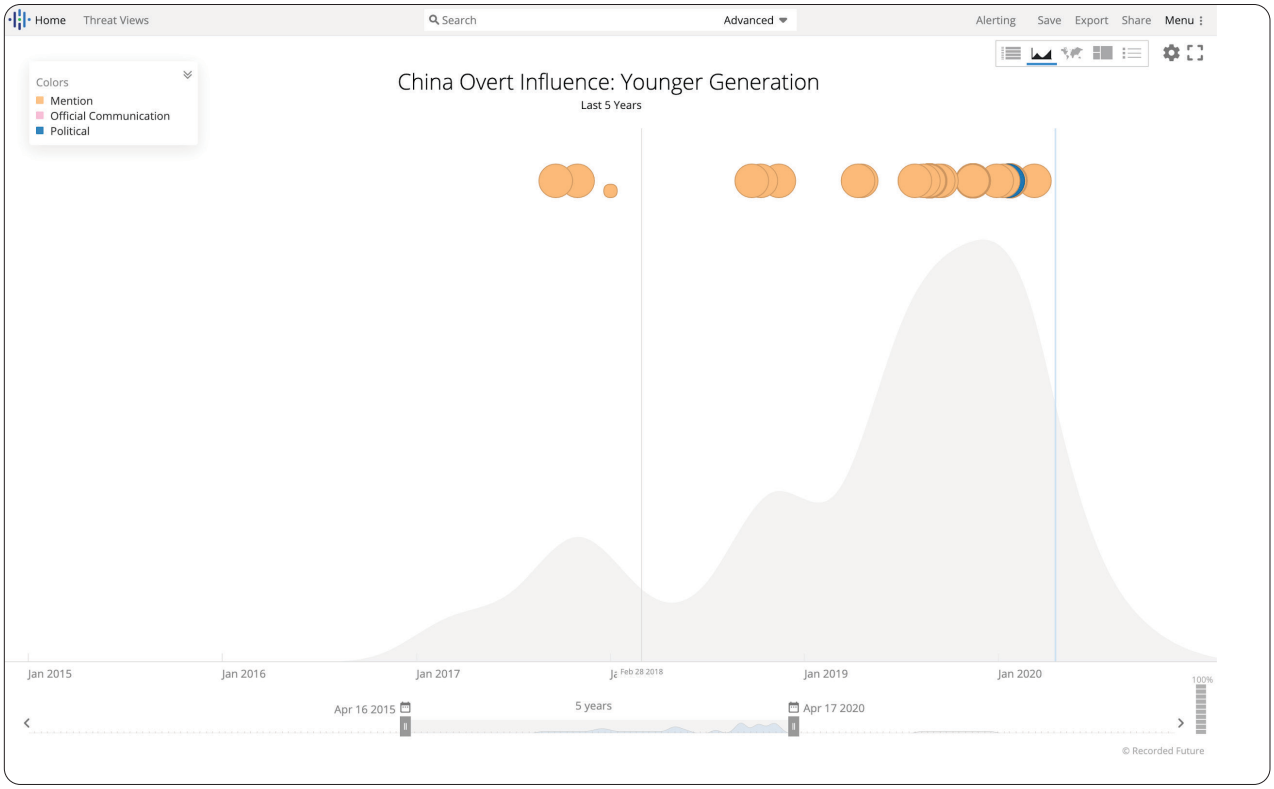
In terms of emerging trends in overt influence by state media, we believe that two factors will be key in the coming years: first, the increased targeting of the younger generation of Taiwanese internet users, and second, the state media's leveraging and amplification of false or biased content from social media and content farms.

Increased Targeting of Taiwanese Youth

Recorded Future observed a steady rise of references to Taiwanese "youth" and "young people" from the same set of accounts over the past five years, with a spike in references in the past year, peaking right before the January 2020 Taiwan elections. Most references centered around career opportunities and testimonies offered by young Taiwanese that have found success in mainland China.

Immediately following the January 2020 re-election of President Tsai, PRC state media Xinhua News Agency published a statement on social media made by Taiwan Affairs Office spokesperson Ma Xiaoguang, stating that "[...] young people on both sides of the strait should communicate more and more. We will never give up on the Taiwanese young people. We will continue to introduce a series of policies through continuous exchanges. The measures will create conditions for cross-strait youth to increase mutual understanding, improve the correct understanding of cross-strait relations, and promote a more objective and correct understanding of the mainland."

While these posts account for a small subset of the posts mentioning Taiwan, we assess that this may indicate that the Chinese state has realized the deciding role that the younger generation of Taiwanese voters is increasingly playing in public opinion and elections.



References to Taiwan's "youth" or "young people" by Chinese state-affiliated Twitter accounts. (Source: Recorded Future)

Leveraging and Amplifying Social Media and Content Farms

Not only do both Taiwanese and Chinese content farms copy content originating from Chinese state media, but investigations have also shown that state media reference and amplify fake or biased content that originates from social media and content farms.

Examples include the 2018 Banana Crisis, during which Xinhua News referenced "Taiwanese public opinion," saying that "deteriorating relations with mainland China brought on by the current administration" was one of the main drivers of plunging banana prices. The Xinhua article was further shared by Chinese content farms including KKNews. Investigative news outlet The Reporter later discovered that the false information had originated from the Taiwanese content farm Mission and morphed as it was shared and copied between anti-DPP Facebook groups and different content farms. A false news story smearing President Tsai published by the Global Times had followed a similar creation and dissemination process and been shared by numerous content farms.

Hong Kong Protests

Between September 21, 2019 and March 20, 2020, Recorded Future observed approximately 230,000 references to Hong Kong protests, an 11.9% drop from the approximately 261,000 references observed in the prior six months (March 21 to September 20, 2019). However, it is worth noting that the first mentions appeared in June 2019, when the protests started. Of the 228,000 references, 692 mentions were related to "disinformation," "fake news," or "influence operations." Much of the reporting was focused on influence operations — some attributed to the Chinese government — carried out on social media (such as Twitter, Facebook, and YouTube), which Recorded Future assesses will continue to be a common TTP employed by Chinese state-sponsored groups.

We highlight two new TTPs observed in the past six months that have been employed by Chinese state-backed groups or groups that are supportive of the state: first, the crowd-sourced doxxing of anti-government protesters, and second, social media "rallies" to support Hong Kong police and authorities, and the Chinese state. Recorded Future assesses that these are likely to become regularly deployed tools in Chinese influence operations due to the general rise of Chinese grassroot patriotism and national pride that are the driving forces behind these campaigns.

Crowd-Sourced Doxxing of Protestors

Since August 2019, Recorded Future has observed multiple websites and Telegram channels or groups created for the purpose of "doxxing" anti-government protesters, publicly revealing their PII and possibly exposing them to cyberbullying or other malicious targeting. These websites collect submissions of doxxing information via an official contact email and publish doxxed profiles in well-designed, uniform templates without revealing their sources. In this report, we focus on two of the biggest doxxing websites: HKLeaks and Hong Kong Mob.

HKLeaks

Original Domain	*hkleaks[.]org* (Registered on August 15, 2019)
Active Domain(s)	*hkleaks[.]pk*, *hkleaks[.]ml*
Contact Email(s)	hkleaks@yandex.com
Related Telegram Accounts[5]	@hkleaks, @hongkong_nes

HKLeaks is the most prominent and widely reported doxxing site targeting anti-government protesters. It has been referenced by Chinese state media and foreign news outlets alike. The site has used at least 12 known top-level domains (full list in Appendix A) since its creation, likely to avoid takedown requests by Hong Kong authorities, as it is illegal to disclose certain personal details of an individual without their consent.

[5] Telegram accounts that are possibly managed by the same actors or majorly promote content from the specific doxxing site.

HKLeaks includes pages that "debunk (anti-government) rumors," list out entities branded as "accomplices of protesters" (including churches, restaurants, corporations, and schools), and break down doxxed targets into seven different categories. Doxxed targets include eight teachers that are seen as supporters of the protests (such as the principal of the Chinese University of Hong Kong), 61 journalists and editors of Apple Daily (one of Hong Kong's biggest newspapers), 23 individuals who allegedly doxxed the Hong Kong police, numerous pro-democracy lawmakers and opinion leaders, and more than 900 protesters. A doxxed profile would include a headshot and information such as the individual's full name, current occupation, date of birth, telephone numbers, Facebook accounts, address, and a brief description of their "misdeeds."

According to data from social media monitoring platform CrowdTangle, as of November 2019, more than two million people follow Facebook pages that have shared HKLeaks's posts. HKLeaks is also promoted by Twitter accounts, Telegram groups and channels, and Weibo accounts.

The doxxing has real-life consequences for some of the victims — a female reporter from Apple Daily, for instance, received hundreds of threatening calls. Anecdotal evidence presented by some of the victims allege that authorities from mainland China may be involved. A victim told AFP that he gave a "fake address I've never given to anyone" to Chinese police while he was questioned at the border when returning to Hong Kong from a business trip in mainland China in August, which showed up as his address on HKLeaks. Another victim told Apple Daily that his photo on the website was the photo he used on his China travel card.

While we are unable to attribute the creation and management of the site to an individual or group of individuals, we assess that HKLeaks is almost certainly the result of a highly coordinated effort and heavy resource investment.

- The continuous curation of doxxing information and production of customized, professional-quality graphics over a period of months show a sustained resource investment.

- The constant shift of domains, the use of bulletproof hosting, and the use of anonymous registration indicate an intent to evade takedown and prosecution. A prominent message on the top of the homepage reads, "We declare that this site will never shut down!"
- HKLeaks has been promoted on social media by accounts similar to those taken down by platforms for coordinated inauthentic behavior linked to state-backed actors. Some social media accounts were created shortly before the website was created in August 2019; others were old, idle accounts that were revived around the same time.

Screenshot of HKLeaks's homepage. (Source: HKLeaks)

Hong Kong Mob

Original Domain	*hongkongmob[.]com*
Active Domain(s)	No longer active
Contact Email(s)	hongkongmob@yandex[.]com, hongkongmob@protonmail[.]com, hongkongmob@163[.]com
Related Telegram Accounts	@hongkongmob, @hongkongmobchannel, @Tearmask

Hong Kong Mob is a doxxing site that provides cash rewards to people who provide either new doxxing targets or information on existing targets. Individuals can submit new doxxing targets via the official contact email address, and can provide information of existing targets through an online form on the website.

Information requested includes Facebook and other social media accounts, and the misdeeds of the target. The first person to provide "useful information" will receive the reward; if multiple people provide useful information, the cash reward would be split among the individuals. The website accepts donations for its cash reward fund.

While Hong Kong Mob is no longer active, the most recent capture from WayBack Machine on January 14, 2020 shows a banner on the homepage stating that 62 protesters have been doxxed, 46 doxxing targets are outstanding, and 78,019 HKD (approximately $10,048 USD) worth of cash rewards have been awarded.

Hong Kong Mob also includes a page that lists out links to similar pro-Hong Kong government and anti-protester websites, Telegram groups and channels, and Facebook groups and pages.

According to its "About Us" page, the website was created by two groups: "Global Volunteers Against Hong Kong's Pro-Independence Mob" (全球反港獨暴徒志願者聯盟), and "Volunteers to Protect Hong Kong" (守護香港志願者聯盟). Recorded Future is unable to attribute these two groups, nor are we able to confirm that they are indeed two separate groups. However, we assess that the actors behind Hong Kong Mobs are likely not Hong Kong natives, but are attempting to pass off as such. Although most of the website is written in traditional Chinese characters (rather than the simplified Chinese characters used by mainland Chinese) and the content mirrors written and spoken Cantonese (which uses distinct characters and wording that is different from the written Chinese of Taiwan and mainland China), some terms and wording used on the website are not commonly used by Hong Kong-born Cantonese speakers.

Screenshot of Hong Kong Mob. (Source: Wayback Machine)

Possible Connections Between Doxxing Websites

Recorded Future has observed similarities between HKLeaks and Hong Kong Mob:

- **Same Hosting Infrastructure**: Both sites were hosted by a Russian bulletproof host service, DDoS-GUARD. Initial domains were hosted on the same IP address block, with hkleaks[.]org hosted on 185.178.208[.]149 and hongkongmob[.]com hosted on 185.178.208[.]143.
- **Same Domain for Contact Email**: Both contact emails are hosted by Russian email service provider Yandex.

While these similarities are not sufficient evidence to support a connection between these two websites, Recorded Future notes that these similarities are not shared with other doxxing websites such as jophk[.]com. We assess that the use of Russian hosting services and email hosts by the websites' creators are likely to maintain anonymity and evade takedown or data disclosure requests from the Hong Kong government or other relevant jurisdictions rather than attempting to pose as Russian actors.

It is also worth noting that many of these doxxing websites and social media groups and channels also promote similar anti-protester, or doxxing, websites and social media channels as resources. We assess that this is due to the political motivation behind the creation of these websites and groups, which eliminates the sense of competition between different websites for online traffic and exposure, as they are all supporting the same cause.

@hkleaks Telegram and Hong Kong Mob link to similar channels and websites. (Source: Telegram, WayBack Machine)

Interactions With State Media

On September 18, 2019, the official Weibo account of CCTV, China's state-owned TV network, published a video showcasing the HKLeaks website, and urged followers to "act together" and "tear off the masks of the rioters." The post was subsequently shared by the Weibo accounts of local Chinese police, local media outlets, branches of Chinese Communist Youth League, and others. While this does not establish a direct connection between doxxing websites such as HKLeaks and the Chinese state, we believe this endorsement by state organizations has, at the very least, supported and encouraged these anti-protester doxxing efforts.

Social Media 'Rallies' to Support Hong Kong Police and Chinese Authorities

China has a history of internet patriotism. The past several years have yielded several examples of Chinese netizens rallying to use VPNs to circumvent the Great Chinese Firewall and leave angry comments on social media accounts of public figures and brands that have "wronged" China and "hurt the feelings of Chinese people." Several online rallies have been observed since the summer of 2019, targeting Hong Kong pro-democracy social media pages and accounts. These rallies differ from usual internet activism from individual Chinese online "patriots," as they involve the congregations of individuals which assume a common identity (other than just patriotism) and often have a fixed start date and time when participants engage in certain online behavior together. Rather than one-off actions of individuals, participation in these rallies is based on and can cultivate a sense of community, rather similar to attending events in the offline world. We highlight two netizen groups that have been most active: "Diba" (帝吧) and "Fangirls" (饭圈女孩).

Diba 'Expeditions'

One of the more coordinated Chinese netizen groups is Diba, a forum with more than 30 million followers on China's largest search engine Baidu, which has organized at least 10 online "expeditions," or "rallies," since 2005. One of Diba's recent expeditions was in 2016 after the election of Taiwanese president Tsai Ing-wen. The group called upon Chinese netizens to flood prominent Taiwan-related Facebook pages with anti-Taiwan independence comments to "show the patriotism of the Chinese youth." Diba users also rallied to flood the Facebook pages of the Swedish national broadcaster SVT and Sweden's Ministry of Foreign Affairs after SVT ran a satirical sketch about Chinese tourists in 2018.

On July 22, 2019, Diba organized its first online rally targeting the Hong Kong protests with the objective to "Support Hong Kong police, maintain rule of law, denounce violence and chaos, and sustain 'one country two systems'." Netizens flooded two pro-democracy Facebook pages with comments supporting the Hong Kong police and "One China." Another rally was planned for the next evening to show support for a pro-China lawmaker in Hong Kong, but was abruptly called off due to "Diba management receiving phone calls from relevant authorities," as outlined in a post on the Diba official Weibo account. No concrete explanations were given but Diba members speculated that the Chinese government may have intervened.

Fangirl 'Rallies'

A new group of Chinese netizens that has sprung out of the Hong Kong protests is called the "fangirls." In China, "fangirls" used to be a slightly demeaning reference to fan groups of celebrities, who have a reputation of pulling crazy stunts to support their "idols" (爱豆) and often get into fierce online arguments with fans of other celebrities. The demographic profile of these fan groups are usually young women born after 1990 (the so-called "post-'90s" generation). As the entertainment industry in China became more competitive, these fan groups have professionalized online rallying and showing support for their celebrities, as these overt expressions of support serve as an indicator for how popular the celebrities are and boosts their careers. On August 14, 2019, numerous groups of fangirls rallied together to show support for a new idol, "Brother China" (阿中哥哥/阿中), an imaginary personification of the Chinese state.

According to local news reports, fangirls had become upset that their beloved celebrities were being attacked online and boycotted by Hong Kong anti-government protesters for speaking out in support of the Hong Kong police and the Chinese state. As a result, fan groups that usually supported different celebrities temporarily put aside their differences and supported the Chinese state. According to Southern Metropolis Daily, a local newspaper, at least 12 different fan groups were created to support the personified "Brother China." Some fan groups had more than 200 people. Within two days, the topic "We all have an idol called Brother China" (我们都有一个爱豆名字叫阿中) was trending on Weibo, and had 790 million views.

The groups were well organized, and had specific teams for image creation, copywriting, translating, and even technical support. They also provided tools and manuals, teaching newcomers how to register for Instagram and Facebook accounts and how to use VPNs. The fangirls not only flooded the social media accounts of pro-China celebrities and public figures with supporting comments, they also flooded Instagram hashtags with pro-China images and memes. Through comments and images, the fangirls created personas for the Chinese state as a male celebrity that "has been active for 5,000 years," "has 1.4 billion fans," "was born into power and influence," but "was bullied by others and lost his status" and had "a son and a daughter that were kidnapped and now refuse to recognize him as their father." These fictional personas of Brother China mirror the common CCP propaganda narratives, including concepts such as the "century of humiliation" and fundamental lore about the Chinese nation.

Instagram comments in support of China (left) and Instagram hashtag #blackcop taken over by pro-China images (right). (Source: Beijing Daily)

Interactions Between Diba and Fangirls

On August 16, 2019, Diba launched its own "Expedition of Patriotic Youths" to support the fangirls' rally. It also promoted the QQ messaging group chat accounts of 17 fangirl groups so that Diba users could join in the ongoing efforts. Diba's call for online patriotism amplified the exposure of the fangirls' online rally, and was shared by many Weibo opinion leaders, including Hong Kong pro-China lawmaker Junius Ho.

Diba's poster for "Expedition of Patriotic Youths" with the captions "Support HK Police, Protect our motherland–CHINA" (left), and real-time updates of the campaign posted on Diba's official Weibo account (right). (Source: Beijing Daily)

Interactions With the Chinese State

State media and state-affiliated organizations played an important role in instigating, encouraging, and promoting the online rallies of fangirls and Diba.

- The August 14 fangirl rally was in part inspired by a Weibo post from CCTV's official account with the title "[Hong Kong Celebrity] Jackson Wang targeted by pro-democracy forces for being patriotic and protecting [the Chinese] flag." The post warned pro-democracy protesters to "immediately stop unlawful, violent behavior, or face dire consequences."

- The fangirl rally was encouraged and promoted by the official Weibo accounts of People's Daily, Communist Youth League, and the Global Times. It was also highlighted on national television, as a segment of CCTV news.
- The August 17 Diba expedition was encouraged and promoted by the official Weibo account of the Communist Youth League.

Recorded Future assesses that the online netizen groups Diba and fangirls are likely grassroot movements that are initiated from the bottom up rather than being directed by the Chinese state. However, it is likely that the Chinese government will start leveraging the existing patriotism and capabilities of these online grassroot groups to promote and defend state interests abroad through explicit direction (such as the phone calls to Diba management by authorities) and implicit nudging (such as encouraging fangirls rallies).

Emerging Chinese TTPs Targeting Taiwan and Hong Kong

Based on the analysis of influence operations targeting the 2020 Taiwan presidential elections and 2019-2020 Hong Kong protests, we have identified the following TTPs employed by Chinese state-sponsored actors or actors supportive of the Chinese state since September 2019.

- Creation of simplified Chinese-, traditional Chinese-, and English-language influence content for dissemination across a wide variety of both traditional social media and messaging applications
- AI-generated content
- Use of social media management software to ease the propagation of influence messaging
- Co-option of witting and unwitting collaborators, such as public figures, politicians, and marketing firms, in spreading Chinese influence information on social media
- Exploitation of the "share" function in LINE to quickly spread misleading, intentionally biased, or false content before it can be countered

- Use and creation of YouTube channels propagating misleading, intentionally biased, or false content designed to look like commentary from domestic citizens
- Employing state-run media to amplify misleading, intentionally biased, or false content
- Microtargeting of specific audiences on other Western social media platforms, such as younger voters in Taiwan
- Crowd-sourced doxxing of anti-government protesters
- Grassroot social media "rallies" to support Chinese state interests

Outlook

Our research here examining recent Chinese state-run influence operations reveals that Chinese operational TTPs, targets, and methodologies continue to evolve.

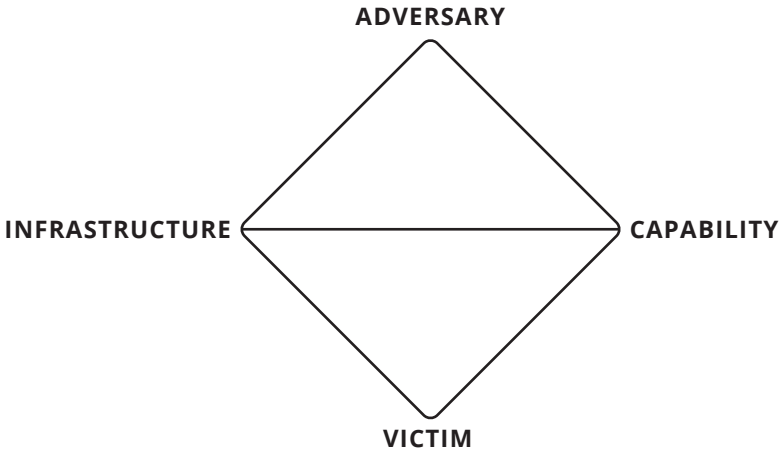
We assess that these campaigns demonstrate that Chinese influence operators are willing to adopt more aggressive tactics that exploit weaknesses in targeted societies or manipulate patriotic sentiments of their own people.

In particular, Chinese influence operations targeting Hong Kong and Taiwan have been able to outmaneuver counter-disinformation efforts in Taiwan and effectively exploit gaps in the terms of service of several social media platforms. The Chinese state also makes use of patriotic individuals and grassroot groups who are both proactive and passionate about their cause, and possess advanced technical and organizing capabilities to execute and sustain influence operations over long periods of time. Another key theme that has surfaced in both the Taiwan and Hong Kong case studies is the role that Chinese state media organizations play in creating, amplifying, and supporting various influence operations that might otherwise not be directly linked to the state.

We expect more of these resources and tactics to be deployed in overseas influence operations on social media platforms over the course of the next year. In particular, automated content creation and dissemination in local languages are likely to be used in targeting foreign audiences for Chinese state interests, especially during sensitive times such as elections and global events. An ongoing example during the current COVID-19 pandemic is the use of botnets to promote Chinese-friendly content in Serbia.

Recorded Future Ontology

Recorded Future's Insikt Group tracks threat activity associated with new and existing threat actor groups, focusing on China, Iran, Russia, and North Korea. Insikt Group only names a new threat actor group or campaign when analysts have data corresponding to at least three points on the Diamond Model of Intrusion Analysis with at least medium confidence, and only when we can point to a handle, persona, person, or organization responsible. We will write about the activity as a campaign in the absence of this level of adversary data. We use the most widely-utilized or recognized name for a particular group when reporting and researching known threat actor groups.



Insikt Group utilizes a simple color plus phonetic naming convention for new threat actor groups or campaigns; we will utilize the most common name when an actor or campaign is already known. The first word in the convention will be a color, currently corresponding to the below, with more color/nation pairings to be added as we identify and attribute new threat actor groups associated with new nations.

Appendix A — HKLeaks Domains

hkleaks[.]org
hkleaks[.]ru
hkleaks[.]kz
hkleaks[.]me
hkleaks[.]pk
hkleaks[.]tj
hkleaks[.]dog
hkleaks[.]news
hkleaks[.]af
hkleaks[.]ml
hkleaks[.]kg
hkleaker[.]net